1. A method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element comprising a sequence of at least one value (a_1,..., a_n) from a predetermined set;

(b) generating a codeword of an error-correcting code for generating the commitment;

(c) constructing a first sequence of coordinate sets (x_i,y_i), for i in {1,...n}, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element and a second value (y_i) corresponding to a symbol in the codeword, wherein the symbol corresponds to the x_ith symbol in the codeword, wherein an order-invariant fuzzy commitment is formed.

2. The method according to claim 1, wherein the representation of the first value in the first sequence of coordinate set is an integer representation.

3. The method according to claim 1, further including outputting the first sequence.

4. The method according to claim 1, further including deriving the first input element from a measurement of a biometric associated with a user.

5. The method according to claim 4, further including selecting the biometric from the group consisting of fingerprint information, retinal scan information, iris scan information, bloodflow-pattern information, thermal imaging information, handwritten-signature dynamics information, physiognomic information, hand geometry information, and voice information.

6. The method according to claim 1, further including adding chaff to the first sequence.

7. The method according to claim 6, further including adding the chaff as sets of pairs of the form (x,y) such that x does not lie in the input sequence and y is generated at random.

8. The method according to claim 6, further including adding the chaff as sets of pairs of the form (x,y) such that one or more values x do lie in the input sequence and y is generated at random.

9. The method according to claim 7, further including reordering the first sequence based upon the first value.

10. The method according to claim 9, further including reordering the first sequence in ascending order based upon the first value.

11. The method according to claim 1, further including applying a bijective function to an input secret to obtain the codeword for the symbol corresponding to the second value.

12. The method according to claim 1, further including decommitting the order-invariant commitment by

receiving a second input element including a second sequence of at least one value $(b_1, ..., b_m)$ from the predetermined set;

receiving the first sequence;

constructing a derived set of values $(X' = x_1', ... , x_m')$ representing respectively the at least one value $(b_1, ..., b_m)$ in the second sequence;

selecting a subset of the coordinate sets $\{(x_i, y_i)\}$ in the first sequence (E) such that for each pair (x',y') in the subset, the first value in the pair (x') lies in the derived set of values (X'); and

applying an error-correcting function to the subset.

13. The method according to claim 12, wherein the error-correcting function includes a Reed-Solomon code.

14. The method according to claim 1, further including selecting a polynomial to generate the codeword.

15. The method according to claim 1, further including utilizing a decodable design for decommiting the order-invariant commitment.

16. The method according to claim 1, further including utilizing a decodable design comprising a design $D_{t,U,\Delta}$ and an algorithm M with running time polynomial in t such that for any $S_i \in D_{t,U,\Delta}$ where $|S_i - S'| \leq \varepsilon$, $M(S') = S_i$, U is a universe, t is a cardinality of the design $D_{t,U,\Delta}$, Δ is a value less than t, such that $|S_i \cap S_j| \leq \Delta$, and the design $D_{t,U,\Delta}$ includes a collection of sets $\{S_1, S_2, ..., S_m\}$.

17. A method for decommitting an order-invariant fuzzy commitment comprising:

receiving a first input element including a sequence of one or more values from a predetermined set ;

receiving an order-invariant fuzzy commitment sequence;

constructing a set of integers having a predetermined number of elements representing respectively values in the first input element;

selecting a subset of the coordinate sets in the first sequence such that the first value in each subset coordinate set corresponds to the first value of at least one coordinate set in the first sequence; and

applying an error-correcting function to the subset.

18. A method for creating a reordering-tolerant fuzzy commitment comprising:

(a) receiving a first input element A including a first sequence of at least one value;

(b) generating a first codeword c of an error-correcting code for the commitment;

(c) constructing a sequence E of one or more data elements responsive to the first input element A and the error-correcting code c;

(d) outputting the sequence E;

(e) receiving a second input element B including a second sequence of at least one value and the sequence E, wherein the second sequence has a number of elements m;

(f) applying a function d responsive to the second input element B and the sequence E, wherein the function yields as output a value of a second codeword ($c' = d(B,E)$), the function having a property such that $d(V,E) = c$ for at least one possible value of V, where V comprises a third sequence having a number of elements m_V, wherein the at least one value of the first sequence differs from the at least one value of the third sequence in at least $m_V/2$ values; and

(g) outputting the second codeword c'.

19. A method for generating an order invariant fuzzy commitment of an item of information, comprising:

receiving a first set of elements; and

selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item.

20. The method according to claim 19, further including inserting chaff points that form a part of the commitment of the item.

21. The method according to claim 19, further including

receiving a second set of elements; and

selectively decommitting the item based upon a level of overlap of the first and second sets of elements.

22. The method according to claim 21, further including determining the polynomial from the second set of elements if the level of overlap is greater than a predetermined threshold.

23. The method according to claim 21, further including utilizing an error-correcting code for determining the polynomial.

24. The method according to claim 23, further including utilizing a Reed-Solomon error detecting code.

25. The method according to claim 19, wherein the first set of elements corresponds to a biometric template.

26. The method according to claim 19, further including utilizing a decodable design to decommit the item, wherein the decodable design includes constituent pairs of sets having a level of overlap less than a predetermined level.

27. The method according to claim 19, further including hiding the first set of elements in a target set containing a plurality of elements selected from a field.

28. The method according to claim 27, further including projecting the first set of elements onto the target set.

29. A system for generating an order-invariant fuzzy commitment, comprising:

a first input device for receiving first elements of information and providing a first set of elements;

a commitment module for encrypting an item of information over the first set of elements using an order-invariant fuzzy commitment scheme;

a second input device for receiving second elements of information and providing a second set of elements; and

a decommitment module for selectively decrypting the item of information based upon a level of overlap between the first set of elements and the second set of elements.

30. The system according to claim 29, wherein the item of information is a key stored on a server.

31. The system according to claim 30, wherein the commitment of the key is held by the user.

32. The system according to claim 31, wherein the user utilizes the decommited key to authenticate the user to the server.

33. The system according to claim 29, further including a chaff generator module for generating chaff as part of the item commitment.

34. The system according to claim 29, wherein the first elements of information include biometric information.

35. A biometric system, comprising:

a scanner for receiving first biometric information from a user;

a commitment module for generating an order-invariant fuzzy commitment of an item of information over the first biometric information; and

a decommitment module for selectively decommitting the item of information from a level of overlap between the first biometric information and second biometric information.

36. The system according to claim 35, wherein the scanner includes a device for receiving biometric information from the group consisting of fingerprint information, retinal scan information, iris scan information, bloodflow-pattern information, thermal imaging information, handwritten-signature dynamics information, physiognomic information, hand geometry information, and voice information.

37. The system according to claim 35, further including a chaff generator module for adding chaff to the commitment.

38. A computer readable medium, comprising code for enabling the steps of:

(a) receiving a first input element comprising a sequence of at least one value from a predetermined set;

(b) generating a codeword of an error-correcting code; and

(c) constructing a first sequence of coordinate sets, each of the coordinate sets having a first value corresponding to a representation of an associated one of the at least one value of the first input element and a second value corresponding to a symbol in the codeword, wherein the symbol is associated with the corresponding first value.

39. The computer readable medium according to claim 38, further including code for enabling the steps of

receiving a second input element including a second sequence of at least one value from the predetermined set;

receiving the order-invariant fuzzy commitment;

constructing a set of values representing respectively the values in the second sequence;

selecting a subset of the coordinate sets in the first sequence such that the first value in each subset coordinate set corresponds to the first value of at least one coordinate set in the first sequence; and

applying an error-correcting function to the subset.

40. A method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one value (a_1,..., a_n) from a predetermined set (F);

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets (x_i,y_i), for i in {1,...k} for integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (y_i) corresponding to a symbol in the codeword (c), wherein the symbol is selected in a manner responsive to the first value x_i, wherein an order-invariant fuzzy commitment is formed.

41. A method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one value (a_1,..., a_n) from a predetermined set (F);

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in {1,...,k} for integer k > 0, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (z_i) constructed in a manner responsive to a pattern of occurrence of the associated one (a_i) of the at least one value of the first input element (A) in the sequence (a_1,..., a_n) and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set (x_i and z_i), wherein an order-invariant fuzzy commitment is formed.

42. The method according to claim 41, further including decommitting the order-invariant commitment by

receiving a second input element (B) including a second sequence of at least one value (b_1, ..., b_m) from the predetermined set (F);

receiving the first sequence (E);

constructing a derived set of values (X' = x_1', ... , x_m') representing respectively the at least one value (b_1, ..., b_m) in the second sequence (B);

selecting a subset (E') of the coordinate sets {(x_i, y_i)} in the first sequence (E) such that for each pair (x',z',y') in the subset (E'), the first value in the pair (x') lies in the derived set of values (X'); and

applying an error-correcting function to the subset (E').

43. A method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one value (a_1,..., a_n) from a predetermined set;

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in {1,…,k} for integer k > 0, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (z_i) constructed in a manner responsive to information in the first input element (A), and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values (x_i and z_i) of the coordinate set, wherein an order-invariant fuzzy commitment is formed.

44. The method according to claim 43, further including decommitting the order-invariant commitment by

receiving a second input element (B) including a second sequence of at least one value (b_1, ..., b_m) from the predetermined set (F);

receiving the first sequence (E);

constructing a derived set of values (X' = x_1', , x_m') representing respectively the at least one value (b_1, ..., b_m) in the second sequence (B); and

selecting a subset (E') of the coordinate sets {(x_i, y_i)} in the first sequence (E) such that for each pair (x',z',y') in the subset (E'), the first value in the pair (x') lies in the derived set of values (X'); and

applying an error-correcting function to the subset (E').

45. A method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one pair of values (a_1,w_1), (a_2,w_2),,..., (a_n,w_n) wherein each of the at least one a_i values is from a first predetermined set (F) and each of the at least one w_i values is from a second predetermined set (G);

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in $\{1,\ldots,k\}$ for integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one $((a_i,w_i))$ of the at least one pair of values of the first input element (A) and a second value (z_i) constructed in a manner responsive to an associated one $((a_i,w_i))$ of the at least one value of the first input element (A) in the sequence (a_1,w_1), (a_2,w_2),,..., (a_n,w_n) and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set (x_i and z_i), wherein an order-invariant fuzzy commitment is formed.